

## Scenario: Site-to-Site VPN Configuration

---

This chapter describes how to use the adaptive security appliance to create a site-to-site VPN.

Site-to-site VPN features provided by the adaptive security appliance enable businesses to extend their networks across low-cost public Internet connections to business partners and remote offices worldwide while maintaining their network security. A VPN connection enables you to send data from one location to another over a secure connection, or tunnel, first by authenticating both ends of the connection, and then by automatically encrypting all data sent between the two sites.

This chapter includes the following sections:

- [Example Site-to-Site VPN Network Topology, page 7-1](#)
- [Implementing the Site-to-Site Scenario, page 7-2](#)
- [Configuring the Other Side of the VPN Connection, page 7-13](#)
- [What to Do Next, page 7-14](#)

## Example Site-to-Site VPN Network Topology

[Figure 7-1](#) shows an example VPN tunnel between two adaptive security appliances.

**Figure 7-1**      *Network Layout for Site-to-Site VPN Configuration Scenario*



Creating a VPN site-to-site deployment such as the one in [Figure 7-1](#) requires you to configure two adaptive security appliances, one on each side of the connection.

## Implementing the Site-to-Site Scenario

This section describes how to configure the adaptive security appliance in a site-to-site VPN deployment, using example parameters from the remote-access scenario shown in [Figure 7-1](#).

This section includes the following topics:

- [Information to Have Available, page 7-3](#)
- [Configuring the Site-to-Site VPN, page 7-3](#)

## Information to Have Available

Before you begin the configuration procedure, obtain the following information:

- IP address of the remote adaptive security appliance peer
- IP addresses of local hosts and networks permitted to use the tunnel to communicate with resources at the remote site
- IP addresses of remote hosts and networks permitted to use the tunnel to communicate with local resources

## Configuring the Site-to-Site VPN

This section describes how to use the ASDM VPN Wizard to configure the adaptive security appliance for a site-to-site VPN.

This section includes the following topics:

- [Starting ASDM, page 7-3](#)
- [Configuring the Adaptive Security Appliance at the Local Site, page 7-5](#)
- [Providing Information About the Remote VPN Peer, page 7-6](#)
- [Configuring the IKE Policy, page 7-8](#)
- [Configuring IPsec Encryption and Authentication Parameters, page 7-9](#)
- [Specifying Hosts and Networks, page 7-10](#)
- [Viewing VPN Attributes and Completing the Wizard, page 7-12](#)

The following sections provide detailed instructions for how to perform each configuration step.

## Starting ASDM

This section describes how to start ASDM using the ASDM Launcher software. If you have not installed the ASDM Launcher software, see [Installing the ASDM Launcher, page 4-5](#).

If you prefer to access ASDM directly with a web browser or using Java, see [Starting ASDM with a Web Browser, page 4-7](#).

To start ASDM using the ASDM Launcher software, perform the following steps:

- 
- Step 1** From your desktop, start the Cisco ASDM Launcher software.  
A dialog box appears.



- Step 2** Enter the IP address or the hostname of your adaptive security appliance.
- Step 3** Leave the Username and Password fields blank.



---

**Note** By default, there is no Username and Password set for the Cisco ASDM Launcher.

---

- Step 4** Click OK.
- Step 5** If you receive a security warning containing a request to accept a certificate, click **Yes**.

The ASA 5580 checks to see if there is updated software and if so, downloads it automatically.

The main ASDM window appears.

The screenshot displays the Cisco ASDM 6.1 for ASA interface for device 172.23.204.72. The main window is divided into several sections:

- Device Information:**
  - Host Name: asdmfull.ciscoasa.com
  - ASA Version: 8.1(2)
  - ASDM Version: 6.1(5)
  - Firewall Mode: Routed
  - Environment Status: OK
  - Device Uptime: 41d 3h 57m 23s
  - Device Type: ASA 5580 40
  - Context Mode: Single
  - Total Flash: 1024 MB
- Interface Status:**

Interface	IP Address/Mask	Line	Link	Kbps
1	no ip address	up	up	0
dmz	192.168.1.1/25	down	down	0
inside	172.23.204.72/24	up	up	4
outside	10.10.20.104/24	up	up	0
- VPN Sessions:**
  - IPSec: 0
  - Clientless SSL VPN: 0
  - SSL VPN Client: 0
- System Resources Status:**
  - Total Memory Usage: 4,000 MB
  - Total CPU Usage: 0%
  - Core Usage: 0%
- Traffic Status:**
  - Connections Per Second Usage: Graph showing 0 connections per second for UDP, TCP, and Total.
- Latest ASDM Syslog Messages:**

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina	Description
6	Nov 19 2008	17:55:30	302010					3 in use, 10 most used
6	Nov 19 2008	17:54:40	302016	5.5.5.1	1050	10.10.20.104	3522	Teardown UDP connection 13048 for outside:5.5.5.1/1050 to identity:10.10.20.104/3522
6	Nov 19 2008	17:52:39	110003	10.10.20.104	3522	5.5.5.1	1050	Routing Failed to locate next hop for UDP from identity:10.10.20.104/3522 to outside:5.5.5.5
6	Nov 19 2008	17:52:39	302015	5.5.5.1	1050	10.10.20.104	3522	Bulk outbound UDP connection 13048 for outside:5.5.5.1/1050 (5.5.5.1/1050) to identity:

## Configuring the Adaptive Security Appliance at the Local Site



### Note

The adaptive security appliance at the first site is referred to as Security Appliance 1 in this scenario.

To configure the Security Appliance 1, perform the following steps:

**Step 1** In the main ASDM window, choose the **IPsec VPN Wizard** option from the Wizards drop-down menu. ASDM opens the first VPN Wizard screen.

In Step 1 of the VPN Wizard, perform the following steps:

- a. In the VPN Tunnel Type area, click the **Site-to-Site** radio button.



---

**Note** The Site-to-Site VPN option connects two IPsec security gateways, which can include adaptive security appliances, VPN concentrators, or other devices that support site-to-site IPsec connectivity.

---

- b. From the VPN tunnel Interface drop-down list, choose **Outside** as the enabled interface for the current VPN tunnel.



- c. Click **Next** to continue.
- 

## Providing Information About the Remote VPN Peer

The VPN peer is the system on the other end of the connection that you are configuring, usually at a remote site.



---

**Note** In this scenario, the remote VPN peer is referred to as Security Appliance 2.

---

In Step 2 of the VPN Wizard, perform the following steps:

- 
- Step 1** Enter the Peer IP Address (the IP address of Security Appliance 2, in this scenario 209.165.200.236) and a Tunnel Group Name (for example “Cisco”).
- Step 2** Specify the type of authentication that you want to use by selecting one of the following authentication methods:
- To use a static preshared key for authentication, click the **Pre-Shared Key** radio button and enter a preshared key (for example, “Cisco”). This key is used for IPsec negotiations between the adaptive security appliances.



---

**Note** When using preshared key authentication, the Tunnel Group Name must be the IP address of the peer.

---

- To use digital certificates for authentication, click the **Certificate** radio button, choose the certificate signing algorithm from the Certificate Signing Algorithm drop-down list, and then choose a preconfigured trustpoint name from the Trustpoint Name drop-down list.

If you want to use digital certificates for authentication but have not yet configured a trustpoint name, you can continue with the Wizard by using one of the other two options. You can revise the authentication configuration later using the standard ASDM screens.

- Click the **Challenge/Response Authentication** radio button to use that method of authentication.



**Step 3** Click **Next** to continue.

---

## Configuring the IKE Policy

IKE is a negotiation protocol that includes an encryption method to protect data and ensure privacy; it also provides authentication to ensure the identity of the peers. In most cases, the ASDM default values are sufficient to establish secure VPN tunnels between two peers.

In Step 3 of the VPN Wizard, perform the following steps:

**Step 1** Click the Encryption (DES/3DES/AES), authentication algorithms (MD5/SHA), and the Diffie-Hellman group (1/2/5) used by the adaptive security appliance during an IKE security association.

**Note**

---

When configuring Security Appliance 2, enter the exact values for each of the options that you chose for Security Appliance 1. Encryption mismatches are a common cause of VPN tunnel failures and can slow down the process.

---

**Step 2** Click **Next** to continue.

---

## Configuring IPsec Encryption and Authentication Parameters

In Step 4 of the VPN Wizard, perform the following steps:

- 
- Step 1** Choose the encryption algorithm (DES/3DES/AES) from the Encryption drop-down list, and the authentication algorithm (MD5/SHA) from the Authentication drop-down list.



- Step 2** Click **Next** to continue.
- 

## Specifying Hosts and Networks

Identify hosts and networks at the local site that are permitted to use this IPsec tunnel to communicate with hosts and networks on the other side of the tunnel. Specify hosts and networks that are permitted access to the tunnel by clicking **Add** or **Delete**. In the current scenario, traffic from Network A (10.10.10.0) is encrypted by Security Appliance 1 and transmitted through the VPN tunnel.

In addition, identify hosts and networks at the remote site to be allowed to use this IPsec tunnel to access local hosts and networks. Add or remove hosts and networks dynamically by clicking **Add** or **Delete** respectively. In this scenario, for Security Appliance 1, the remote network is Network B (10.20.20.0), so traffic encrypted from this network is permitted through the tunnel.

In Step 5 of the VPN Wizard, perform the following steps:

- 
- Step 1** In the Action area, click the **Protect** radio button or **Do Not Protect** radio button.
  - Step 2** Enter the IP address of local networks to be protected or not protected, or click the ellipsis (...) button to select from a list of hosts and networks.
  - Step 3** Enter the IP address of remote networks to be protected or not protected, or click the ellipsis (...) button to select from a list of hosts and networks.



- Step 4** Click **Next** to continue.
-

## Viewing VPN Attributes and Completing the Wizard

In Step 6 of the VPN Wizard, review the configuration list for the VPN tunnel you just created.



If you are satisfied with the configuration, click **Finish** to apply the changes to the adaptive security appliance.

If you want the configuration changes to be saved to the startup configuration so that they are applied the next time the device starts, from the File menu, click **Save**.

Alternatively, ASDM prompts you to save the configuration changes permanently when you exit ASDM.

If you do not save the configuration changes, the old configuration takes effect the next time the device starts.

This concludes the configuration process for Security Appliance 1.

For information about verifying or troubleshooting the configuration for the Site-to-Site VPN, see the section “Troubleshooting the Security Appliance” in the *Cisco Security Appliance Command Line Configuration Guide*. For specific troubleshooting issues, see the Troubleshooting Technotes at the following location:

[http://www.cisco.com/en/US/products/ps6120/prod\\_tech\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps6120/prod_tech_notes_list.html)

## Configuring the Other Side of the VPN Connection

You have just configured the local adaptive security appliance. Next, you need to configure the adaptive security appliance at the remote site.

At the remote site, configure the second adaptive security appliance to serve as a VPN peer. Use the procedure you used to configure the local adaptive security appliance, starting with “Configuring the Adaptive Security Appliance at the Local Site” section on page 7-5 and finishing with “Viewing VPN Attributes and Completing the Wizard” section on page 7-12.



---

**Note**

When configuring Security Appliance 2, use the same values for each of the options that you selected for Security Appliance 1, with the exception of local hosts and networks. Mismatches are a common cause of VPN configuration failures.

---

For information about verifying or troubleshooting the configuration for the Site-to-Site VPN, see the section “Troubleshooting the Security Appliance” in the *Cisco Security Appliance Command Line Configuration Guide*. For specific troubleshooting issues, see the Troubleshooting Technotes at the following location:

[http://www.cisco.com/en/US/products/ps6120/prod\\_tech\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps6120/prod_tech_notes_list.html)

## What to Do Next

If you are deploying the adaptive security appliance only in a site-to-site VPN environment, then you have completed the initial configuration. In addition, you may want to consider performing some of the following steps:

To Do This...	See...
Refine configuration and configure optional and advanced features	<i>Cisco Security Appliance Command Line Configuration Guide</i>
Learn about daily operations	<i>Cisco Security Appliance Command Reference</i>  <i>Cisco Security Appliance Logging Configuration and System Log Messages</i>

You can configure the adaptive security appliance for more than one application. The following sections provide configuration procedures for other common applications of the adaptive security appliance:

To Do This...	See...
Configure an SSL VPN for the Cisco AnyConnect software client	<a href="#">Chapter 5, “Scenario: Configuring Connections for a Cisco AnyConnect VPN Client”</a>
Configure a clientless (browser-based) SSL VPN	<a href="#">Chapter 6, “Scenario: SSL VPN Clientless Connections”</a>
Configure a remote-access VPN	<a href="#">Chapter 8, “Scenario: IPsec Remote-Access VPN Configuration”</a>